基于数字化校园的一卡通系统的安全性探讨

王学敏
(厦门大学 信息与网络中心,自动化系 福建 厦门 361005)

摘要:校园一卡通是数字化校园建设重要组成部分和基础工程,为数字化校园提供了全面的数据采集网络平台。本文将结合一卡通系统的建设,重点探讨一卡通的安全性。

关键词:校园一卡通;数字化校园;安全性
中图分类号:TP393　　文献标识码:A　　文章编号:1009-3044(2007)12-21541-01

The Security of the E Card System in the Digital Campus

WANG Xue-min
(Information and Network Center of XiaMen University,Automation Department,Xiamen 361005,China)

Abstract:The E-Card System is foundation of the construction of digital campus.It provides the network platform throught which all kinds of data are collected,this essay illustrates the security of the E-Card system of digital campus.

Key words:E Card System;Digital Campus;System Surity

1 数字化校园与校园一卡通

随着中国高等教育信息化建设的蓬勃发展,现在各个高校更重视全面发展‘数字化校园’的建设。希望能通过‘数字化校园”整合校园内各信息管理系统,使各信息系统能够在统一的数据平台实现信息共享,实现校园的信息共享和资源合理分配,从而提高教学质量、科研水平和管理水平。而校园一卡通系统是数字化校园的基础工程和重要的有机组成部分,旨在为广大师生员工的教学、科研和生活提供方便、快捷的电子化服务。校园一卡通系统是以软件集成为主、硬件集成为辅的综合信息集成系统,构建在数字化校园之上的统一身份认证、中央共享数据库、统一信息门户等基础平台,与学校其它业务管理信息系统紧密结合,实现数据共享和交换,组成数字化校园的重要信息采集网络,为学校提供实时可靠的信息来源和决策依据。

2 校园一卡通的系统安全体系

校园一卡通系统中所传输的数据的特殊性——金融交易数据,以及其它 MIS 数据、身份信息、认证信息、密钥传递等,因此对整个系统的安全性要有全面的考虑。下面我们将从不同的角度的探讨系统的安全性。

2.1 网络安全

在高校的局域网中,用户量大,病毒也多,而且扩散快。而对于一卡通这对网络安全要求比较高而言,如果建立在局域网上,那么势必导致较高风险,所以采用一卡通专网是比较安全的。该一卡通系统按其服务对象来分可分为:银行接入区、核心服务器区、对外服务区和用户服务区。银行与“一卡通”专用主干网之间是互连采用租用 DDN 专线接入的方式。连接设备基本采用路由器+网关隔离机进行互连。在路由器上配置访问控制列表(ACL),提供与银行间的网络的安全隔离。网关隔离机上配置双网卡,一端连接外围,一端连接校内网,保证与银行互连在数据链路层进行安全隔离。一卡通专网与校园网的唯一接口处(用于校园网用户通过 Web 方式从校园网直接访问一卡通系统的 Web 服务器)配置高性能的防火墙并虚拟其地址。其总体逻辑拓扑结构如下图所示。

2.2 服务器的安全

一卡通系统的核心服务器(一卡通身份认证服务器、核心数据库服务器)采用的是 Sun Fire V440 和 Sun Fire V880 的高性能服务器,并双机热备,即当一台服务器停机,另一台机器马上进行切换。保障系统的正常稳定的运行。服务器机房为专用机房,ups 断电保护,24 小时恒温,气体消防,防静电处理等。

2.3 终端设备安全

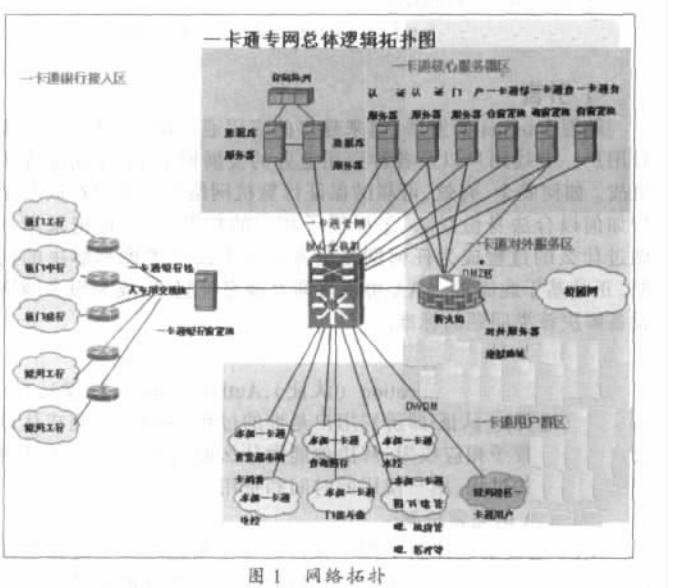

图 1　网络拓扑

一卡通网内的各个终端设备都有唯一的标识号,定位于限定的组织结构以防止设备被随意更换;设备断电后再开机,必须经授权才能再使用。收费终端采用 UPS 供电以及无源存储保护数据技术,正常情况下,终端数据信息均具有代码标识,实时上传结算;异常发生时,启动收费终端的数据分析功能,迅速查出数据出错源,通过底层数据还原校验予以纠正。

2.4 操作系统与数据库系统的安全

一卡通系统采用 SUN Solaris 操作系统以及 Oracle 作为整个系统的后台中心数据库。Oracle10.0 数据库平台被广大金融、证券、邮电业务处理系统所采用其安全性可靠,达到美国国防部安全标准 C2 级。其架构在公认系统级数据安全的基础上,Oracle 数据库本身使用了多种手段来加强数据库的安全性,常见的就有密码、角色、权限等等。而且,后台中心数据库采用双机热备份来保证系统安全稳定运行,使终端设备的批量交易数据能够实时回传。中心数据存储采用双重保障机制,一方面通过磁盘阵列柜进行交易数据的实时备份;另一方面通过磁带机对每天日结后的数据进行备份保存,绝对保证数据存储的完备、安全、可靠。同时,在交易终端,也采取多种措施防止交易数据丢失。如在网路不通的情况下,终端机可以脱网运行,终端本身能够存储 2 万多笔脱机交易流水。另外,现场网络的商务网关能够存储多达 10 万笔的交

(下转第 1544 页)

收稿日期:2007-05-22
作者简介:王学敏(1978-),男,硕士研究生,工程师,主要研究领域:系统集成,办公自动化系统等。

802.1x 协议为二层协议,不需要到达三层,而且接入层交换机无需支持 802.1q 的 VLAN,对设备的整体性能要求不高,可以有效降低建网成本;通过组播实现,解决其他认证协议广播问题,对组播业务的支持性好; 业务报文直接承载在正常的二层报文上;用户通过认证后,业务流和认证流实现分离,对后续的数据包处理没有特殊要求。

5.2.2 缺点

需要特定客户端软件;

该协议已经得到了很多软件厂商的重视, 目前微软新版的 windows XP 已经自带 802.1x 客户端软件。

总之,三种认证技术各有优缺点,需要在实际应用中根据每种技术的技术特点和实际情况,综合考虑才会使宽带网络发挥出应有的效益。

参考文献:

[1]糜正琨.等.软交换技术与协议[M].北京:人民邮电出版社,2002:323-325.

[2]曹秀英.等.无线局域网安全系统[M].北京:电子工业出版社,2004:74-77.

[3]李学军.等.宽带 IP 城域网的优化策略与实践[M].北京:人民邮电出版社,2002:122-123.

[4]蔡康.等.IP 宽带业务与运营[M].北京:人民邮电出版社,2003:100-105.

[5][美]Cisco Systems 公司,思科网络技术学院教程:无线局域网基础[M].北京:人民邮电出版社,2005:366-369.

(上接第 1541 页)

易数据,这些设备保证了系统的持续性,同时也为系统的网络恢复提供了足够的时间。

2.5 数据传输的安全

在系统中客户机都是进行过认证,非本系统的客户机无法接入系统。在数据传输时对传输的业务数据通过 DES 用动态密钥进行加密,该动态密钥是每日一变,所以即使通讯包被非法截获截获者也无法解密,更得不到正确数据。

2.6 卡片的安全

采用非接触式 IC 卡作为系统的使用卡,非接触式 IC 卡又称射频卡,是世界上最近几年发展起来的一项新技术,在卡片靠近读写器表面时即可完成卡中的数据的读写操作, 它成功地将射频识别技术和 IC 卡技术结合起来,解决了无源(卡中无电源)和免接触这一难题,是电子器件领域的一大突破,具有以下优点:

(1)可靠性高

非接触式 IC 卡与读写器之间无机械接触, 避免了由于接触读写而产生的各种故障。例如:由于粗暴插卡,非卡外物插入,灰尘或油污导致接触不良等原因造成的故障。此外,非接触式 IC 卡表面无裸露的芯片,无须担心脱落,静电击穿弯曲,损坏等问题,既便于卡片的印刷,又提高了卡片使用的可能性。

(2)操作方便、快捷

由于使用射频通讯技术, 读写器在 10cm 范围内就可以对卡片进行读写,没有插拔卡的动作。非接触式 IC 卡使用时没有方向性,卡片可以任意方向掠过读写器表面,读写时间不大于 0.1 秒,大大提高了每次使用的速度。

(3)安全防冲突

非接触式 IC 卡的序列号是唯一的, 制造厂家在产品出厂前已将此序列号固化,不可更改。世界上没有任何两张卡的序列号会相同。非接触式 IC 卡与读写器之间采用双向验证机制,即读写器验证卡的合法性,同时卡也验证读写器的合法性。非接触式 IC 卡在操作前要与读写器进行三次相互认证,而且在通讯过程中所有数据被加密。卡中各个扇区都有自己的操作密码和访问条件。

另外, 非接触式 IC 卡与读写器之间无机械接触,从而避免了由于接触读写而产生的各种故障。非接触式卡表面无裸露的芯片,无需担心芯片脱落、静电击穿、弯曲损坏等问题。使用时没有方向性,卡可以任意方向掠过读写器表面,避免了接触式读写中由于座口铗小而难以把卡插入的困难。采用双向验证机制,读写器验证 IC 卡的合法性,同时验证读写器合法性,而多数普通有接触式 IC 卡均为单向验证。每张卡均有唯一的序列号。制造厂家在产品出厂前已将序列号固化,不可再更改,该序列号具有唯一性,且卡片上同时印有用户的姓名、性别、照片等个人信息,更加提高了卡片的安全性。

2.7 防病毒系统

采用目前 Symantec AntiVirus Corporate (诺顿杀毒软件企业版本)作为一卡通专网的防病毒系统,作为世界上最优秀的杀毒软件之一,诺顿杀毒企业版能够提供自动杀除桌面系统和网络服务器中的病毒、蠕虫和特洛伊木马并及时发送更新,为客户端提供主动威胁防护,如间谍软件、广告软件和多种黑客工具。为专网中的网关及服务器环境提供内容过滤和垃圾邮件防护,以及提供恶意软件防护,能够做到在每一个网络层提供有效的防护。

诺顿杀毒软件企业版可以在整个一卡通专网内的工作站和网路服务器层提供最佳的多平台病毒防护。能够访问智慧化后端服务以及独有的自动回应机制,可以分析并部署比病毒扩散更快的经过质量测试的对策。即使在受到快速扩散的攻击时面临极大的需求,诺顿的可延伸性后端结构能够确保更快地提供病毒定义码更新。同时诺顿的集中化管理功能使得系统可时时受到保护,使得管理人员可以管理按照逻辑关系组织的客户和服务器,建立、部署和锁定策略和设置,从而保证系统在所有时候都能够保持最新状态,也保证了 DOS、Windows 以及 Netware 服务器和工作站都能够得到更新并且适当配置。

2.8 持卡人的利益保证

对于持卡人而言,他的利益是否能得到保证是考核一卡通的安全性的一重要参数。本校园一卡通系统从以下几个方面做到持卡人的利益保障。

(1)密码限额大额消费启用个人密码:根据持卡人设置,当一次消费或一天消费超过一定额度时,系统将启用个人消费密码。

(2)挂失实时生效:挂失可分为电话语音挂失、圈存机挂失、卡务中心挂失。一经挂失,在各个终端上立即生效。

(3)实时更新黑名单

(4)脱机消费限额:当卡片脱机消费时分别采用不同的限额来启用个人密码、禁止消费从而使丢失但来不及挂失的卡造成的损失最小。

3 结束语

基于校园数字化的一卡通系统是一个管理层次上的系统,系统中涉及到金融、用户、权限、资源等关键且敏感数据,从而一卡通系统的安全体系尤为重要,直接关系到系统的成效以及后续的数字化校园的建设。通过一卡通的安全体系的分析探讨,得到切实可行的安全解决方案,并在我校的一卡通系统中,取得良好的效果。

参考文献:

[1]王爱英.智能卡技术(第 2 版)[M].北京:清华大学出版社,2000.

[2]俞葵,方永胜.基于数字化校园的校园一卡通平台设计[J].运筹与管理,2006,15(3):155-159.

[3]李文琦,郭武.校园一卡通系统安全性能分析[J].网络安全技术与应用,2003,12:44-47.

[4]席琳琳.校园一卡通与数字化校园建设[J].职业教育研究,2005,5:121-122.

[5]苏文胜,马千军.基于数字化校园的校园一卡通构建[J].武汉理工大学学报,2005,27(1):99-101.

[6]刘虎.校园一卡通系统方案设计[J].淮阴工学院学报,2006,15(3):39-42.